2C Incident Response Management

I kritisk infrastruktur

2C Networks Incident Response Management Service

Service Leverance		Standard OnCall	Incident Response	Incident Response Management
Responstid på henvendelse	2 timer	•		
	1 time		•	•
Onsite responstid	Ikke mulig	•		
	4 timer		•	•
Hændelsesanalyse	12 timer[1]		•	•
Indkapsling af hændelse	24 timer[1]			•
Udbedring og genopretning	48 timer[1]			•
Efter-hændelsesanalyse Rapport	5 dage efter genopretning		•	•
Resource location	Remote	•		
	Onsite & Remote		•	•
2C Mgmt escalation	Ikke mulig	•		
	Ja		•	•
Kompetence	Vagthavende	•		
	Vagthavende og prioriteret adgang til relevante specialister		•	•
	Ovenstående + erfaren 2C incident manager			•
Tilgængelighed	Man-Fre, 8-17	•		
	24/7 Support		•	•
Betaling for forbrugt tid	Aftalt timepris	•		
	Aftalt timepris, +100% udenfor normal arbejdstid		•	•
Øvrige services	Udvikling af responsplan			•
	Udvikling af Årshjul			•

Dækningsområde for ovenstående er gældende for Jylland, Fyn, Sjælland. Øvrige landsdele er best effort.

[1] Efter 2C er informeret om hændelse

2C Networks tilgang til Incident Response Management

Proaktiv Forberedelse

- Baseret på jeres netværk udvikler vi en skræddersyet responsplan. Denne plan beskriver trin-for-trin-procedurer for indkapsling, udryddelse og genopretning
- Udvikling af Årshjul med formålet at sikre løbende opfølgning på paratheden af:
    - Identifikation af potentielle trusler og sårbarheder i jeres netværk
    - Ekstern leverandører hvor formålet er at sikre de nødvendige aftaler er på plads med eksterne leverandører og at leverandørerne evner at stå klar til at afdække risiko på tværs af det samlede teknologilandskab
    - Politikker og Procedurer for at sikre etablering af klare retningslinjer for håndtering af sikkerhedshændelser
    - Træning for at uddanne medarbejdere i bedste praksis for cybersikkerhed og regelmæssige øvelser for at teste og forbedre IR-planer

Indkapsling af hændelse

- Hurtig isolering af påvirkede systemer for at forhindre spredning
- Begrænsning af skader og beskyttelse af kritiske data og tjenester

Udbedring og genopretning

- Reparation af skader og gendannelse af data for at sikre optimal drift
- Implementering af opdateringer og forbedrede sikkerhedsforanstaltninger for at forhindre fremtidige hændelser

Hændelsesanalyse

- Hurtig identifikation og analyse af sikkerhedshændelser
- Udvikling af effektive afhjælpningsstrategier for at forhindre fremtidige trusler

Efter-hændelsesanalyse Rapport

- Identifikation af årsager og konsekvenser for at lære af hændelsen
- Anbefalinger til forbedrede sikkerhedsforanstaltninger og fremtidig beredskab